**Crime Mapping and**
**Data Confidentiality Roundtable**
**July 8-9, 1999**
**Sponsored by: National Institute of Justice,**
**Crime Mapping Research Center**

# *Privacy Issues in the Presentation of Geocoded Data*

by
Tom Casady
Chief of Police, Lincoln, Nebraska

Police incident reports—the ubiquitous short form that represents the initial report of a crime or significant police event—are public records virtually everywhere. Other original police reports, such as motor vehicle accident reports, police dispatch records, traffic citations, and arrest reports are commonly declared by law to be public records as well. Anyone with the time and desire can go to their local police department and examine such records. For a small fee, you can obtain a copy of most reports of this type.

Any of these public record reports may contain information that citizens may wish to protect. For example, the police officer's accident report has the drivers' names, dates of birth, addresses, driver's license numbers, automobile license numbers, and telephone numbers. One may jealously guard such information in ordinary circumstances, but after a fender bender it is often a public record available to anyone. The privacy of such information is protected primarily by the cumbersome mechanism for accessing the public record. For the most part, this requires a trip to police headquarters, a hunt for a parking spot, followed by the unparalleled customer service we have come to expect in government offices that enjoy a complete monopoly on the service they provide. As a practical matter, no one just stops in to read reports recreationally. They come only when a specific purpose requires, usually obtaining a copy of an incident report or accident report to accompany an insurance claim.

Although most citizens will do just this at one time or another, for the most part, perusing public record police reports is the pastime of newspaper reporters, claims adjusters, and certain lawyers. These are the people most likely to be populating the lobby of the police records unit, thumbing through the reports on the clipboard. The privacy of otherwise personal information is protected only by the fact that, except for serious incidents or unusual circumstances such as cases involving public figures, these events just aren't newsworthy.

The rather Byzantine process for accessing public record police records has limited the distribution of police reports and the data contained in them. Today, however, the convergence of several technologies is changing this rapidly. First, most police agencies have computerized some or all of these basic records. Traffic accident reports may be stored as digital images, dispatch records created in a computer database, incident reports keystroked into a computerized records management system. Second, the distribution of these electronic records has become comparatively simple. It is not difficult to strip out data fields from the incident report in the police database to HTML screens, to e-mail image file from the accident report to the insurance company, or to post the entire daily dispatch log to the Internet server. In fact, a growing number of police departments are doing just this. Third, the growing use of geographic information systems has vastly improved the ability of the police to provide data and information in a useful and interesting format to the public. Few people are interested in driving to the police station to look over stacks of incident reports, but many people are interested in checking the department's web site and perusing the crimes in their own neighborhood. When crime maps and accompanying data are made available, people will use the information.

Not all of these people have pure motives. Anxious to find your ex-spouse's new address and phone number? Want to track down a borrower in default? Interested in direct mail to solicit new clients from among crime victims? On-line access to crime data is another tool to use in such circumstances. Even perfectly legitimate uses can have undesirable side effects. Looking for a home in a safe neighborhood? Want to make sure your college-bound daughter doesn't rent in a dangerous apartment complex? Thinking about opening another retail outlet in the city? Crime maps provide valuable information in these situations, but can also create a self-fulfilling prophecy, or even contribute to the redlining of neighborhoods with higher frequency of crime. To be sure, when the public has access to information, someone will discover a way to use it for nefarious purposes or its use will have unintended negative impacts.

Another significant concern deals with the accuracy of geocoded data. Police departments using GIS software are geocoding addresses against a street database. Aside from the errors made by officers and clerks in writing and keystroking correct addresses, the geocoding process introduces other sources of location error. Street databases are not always accurate to begin with. Errors aside, commercial street data often omits recently platted streets. Moreover, the geocoding process is inherently inaccurate, since the software is making a "best guess" on where to place the point along a line segment. New streets, similar street names, multiple prefixes and suffixes, and identical street names in separate municipalities may all cause geocoding errors. While software settings can minimize these, squeezing the geocoding parameters too tightly negates its very purpose—speeding and simplifying the process of locating the point.

To make matters worse, geocoding errors are not always easy to spot. It may be rather simple to double check the location of 50 residences of parolees, but it is another matter entirely to perform quality control on the geocoded location of 3,000 burglaries, 5,000 larcenies, 10,000 traffic accidents, and so forth. Except for the smallest files, source data invariably contains location errors, and geocoded data will contain even more. Last year, police officers in Lincoln, Nebraska responded to 140,000 dispatches. If the source data was 100% accurate, and dispatch records were geocoded accurately 99% of the time, 1,400 dots would be misplaced on the resulting map. In reality, geocoded data is not nearly so accurate.

While geocoded data is inherently imprecise, there is little need for concern when large data files are aggregated. A color density map displaying the number of auto thefts per capita within census tracts, for example, tolerates geocoding errors with virtually no impact on the relationships it represents. On the other hand, a single incorrect address or geocoding error in data about registered sex offenders is a major mistake with potentially damaging consequences.

Grappling with the inherent imprecision of geocoding, privacy concerns, the potential for redlining, negative economic impacts, and similar concerns, it will be a challenge to convince police chiefs to move forward with public access to crime maps. The privacy issue of crime mapping boils down to ease of access. Public record information is being made available in a convenient, timely, and useful format. It's no wonder we are worried that people may actually start looking at it. We must remember that distributing this data has tremendous value. Citizens can be informed of risk, motivated to take precautionary measures, aware of trends in the broader community, aroused to action, encouraged to support public policy. Withholding information—or intentionally avoiding technologies that would make access to it simpler, cheaper, and quicker—is an overreaction that is worse than the problem it seeks to prevent or avoid.

Given these issues and concerns, the question arises: *Should professional standards or guidelines be developed for crime mapping as it pertains to privacy and freedom of information issues? If so, what should these standards look like and who should promote them*? At the outset, the standards approach has a certain appeal. Promulgating standards offers the potential establishing an accepted professional practice regarding the release of geocoded data. But the very concept of standards implies the existence of a set of practices upon which there is a reasonable degree of consensus among well-informed practitioners. At the present time, this just does not exist. Crime mapping is still new. Police department's are not at the forefront of Internet distribution of data. Few agencies are grappling with these issues. Agency practice is being reformulated constantly as police departments initiate new applications, exploit opportunities, and encounter problems. State laws vary with regard to what information constitutes a public record. There is scant case law to further define the parameters for redacting data from an electronic data file that would otherwise be contained in a public record report. In sum, the field remains in flux. Attempts to establish and promote standards are unlikely to succeed.

Guidelines, however, are a different matter. The term implies a less certain and more adaptable collection of considerations that may inform or guide others. Guidelines that provide law enforcement agencies with information that may assist them—particularly information that helps them learn from the mistakes made or problems encountered by their counterparts—are more likely to have a positive impact. While the federal government's track record in standard-setting for local law enforcement is not always sterling (NIBRS comes immediately to find), it has an unparalleled ability to disseminate information. Hardly a day goes by that the local police chief is not glancing at an NIJ Research In Brief, the FBI Law Enforcement Bulletin, an OJJDP Fact Sheet, or some other similar publication. Combined with rich Internet resources, the Department of Justice and its subordinate agencies affect practice in significant ways through information. Publishing and publicizing information guidelines concerning confidentiality issues in geocoded data is a service that the Crime Mapping Research Center is in the best position to fill.

What kind of guidelines, pointers, considerations, and cautions are appropriate for police agencies? The answer may still be somewhat unclear, but there are several that can be gleaned from experience:

Public record reports may contain highly personal information. Better access to public records makes it easier for that information to be used in undesirable ways.

Presenting geocoded crime data aggregated into polygons, such as police beats or census tracts protects the identifying information that may be in the source records. See, for example, the Wichita Police Department,

HYPERLINK "http://www.wichitapolice.com/"

When presenting data tables or records to identify geocoded points, police agencies should consider redacting those fields containing personal information such as victims' names, where warranted. See for example, the Lincoln Police Department's approach,

HYPERLINK "http://www.ci.lincoln.ne.us/city/police"

Static maps which are not accompanied by database information or tables pose little risk of identifying specific households or individuals, and still present useful crime pattern information to the public. See, for example, Salinas, California Police Department's maps,

HYPERLINK "http://www.salinaspd.com/maps.html"

Privacy of victims or other individuals can be protected by eliminating exact street addresses in tables or records. This can be accomplished simply by such means as replacing exact street addresses with a block range, or a poloygon feature, such as a police reporting district or census tract.  See, for example, the San Antonio Police Department's site,

HYPERLINK "http://www.ci.sat.tx.us/sapd/maps.htm"

Employ a disclaimer to warn users that some geocoded points may be misplaced.  See, for example, the Sacramento Police Department's disclaimer,

HYPERLINK "http://206.170.172.28/parcels/cdisclaimer.htm"

Most importantly, accept the fact that providing easier access to police data has its downsides.  Ensure that the data being provided is from records that constitute public records in your jurisdiction.  Criticism, liability, or ethical breaches are less likely if only information that is already open and available to the public is provided via GIS maps and related databases.

The most conservative approach would be to avoid any technology that opens access to this public information.  While this reduces some of the risks of disclosure, it is a strategy that carries its own risks in lost opportunity.  Ultimately, the benefits of wider distribution of crime mapping products to the public far outweigh the negatives.  Remember that this information is probably public record data.  If police agencies do not present geocoded crime data on maps, someone else very well may.  Anyone with access to commonly available GIS software and with the capability of obtaining or creating a simple table of incidents can create their own maps.  News media organizations, in fact, have done just that in some places.  See, for example, the CrimeTracker offered by KWTV Channel 9 for the Oklahoma City metropolitan area,

HYPERLINK "http://www.kwtv.com/"

With the rapid development of crime mapping, there has been little opportunity for the natural development of discussion groups, professional associations, conferences, and the other networks that stimulate broader dialog on issues such as privacy concerns with geocoded date.  This is changing quite quickly, however.  As this issue continues to generate thought and discussion, and as more crime analysts and GIS-savvy police executives talk to one another, they will discover that they are not alone.  Other departments are struggling with the same questions, and the same issues are confronting every other industry or service area that holds large amounts of data.  The child support collection agency, school district, register of deeds, motor vehicle department, vital statistics bureau, county appraiser, clerk of the court, and many other public officials possess such data in public records.  Some of these agencies and officials are also beginning to make these records available on the Internet.  They are, or will be, confronting the same issues of privacy vs. access to public records.

Crime mapping and the distribution of mapping products via the Internet is in its youth, and has tremendous potential for public benefit. The evolution of the field mirrors the entrepreneurial spirit that stimulates the Internet in general. New applications are surfacing regularly, and are more current, more interactive, and more informative than the first generation of static crime maps. It would be a mistake to weigh down the dynamic evolution of crime mapping and Internet distribution of information prematurely with standards that are unlikely to succeed in solving the complex issues of privacy versus accessibility.